UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/523,690	02/03/2005	Kazunori Saito	1560-0422PUS1	8523

2292 7590 10/21/2008

BIRCH STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH, VA 22040-0747

EXAMINER	
SCHWARTZ, DARREN B	

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
10/21/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mailroom@bskb.com

Office Action Summary	Application No.	Applicant(s)	
	10/523,690	SAITO, KAZUNORI	
	Examiner	Art Unit	
	DARREN SCHWARTZ	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 August 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5 and 7* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5 and 7* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *02-03-05 07-17-08*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Regarding the Information Disclosure Statement (IDS), the Examiner has signed all PTO-SB08 forms.

2. In light of applicant's cancellation of claim 6, the 35 U.S.C. 101 rejection is withdrawn.

3. Applicant's arguments filed 26 August 2008 have been fully considered but they are not persuasive.

4. Applicant argues that Bates does not have motivation for "judging whether or not an instruction code for calling an instruction code group for executing a predetermined process is associated with the stored branch destination address."

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, Bates teaches "judging whether or not an instruction code for calling an instruction code group for executing a predetermined process is associated with the stored branch destination address" as Bates is directed to a method and apparatus for debugging computer programs that provides means for inserting breakpoints at program logic decision points

that may have caused an event to occur. Such an event may be an unexpected halt, the execution of unexpected program statements, or the assignment to a variable of an unexpected value.

5. Applicant argues that Bates fails to teach "**judging** whether or not an instruction code for calling an instruction code group for executing a predetermined process is associated with the stored branch destination address."

The Examiner disagrees. Applicant's and applicant's representative are reminded that a prior art reference must be considered in its entirety, i.e. as a whole; see W.L. Gore & Associates, Inc. v. Garlock, Inc., 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), cert. denied, 469 U.S. 851 (1984) [MPEP: 2141.02 VI]. Bates teaches "…The method then determines which basic block contains the statement(s) and then determines which blocks control execution of the basic block…" (¶10) and "…The method then determines which basic blocks contain the statements and then determines which blocks control execution of the basic blocks…" (¶11). Therefore, Bates does anticipate the structure of "judgement." As to the claimed limitation "judging **whether or not an instruction code for calling an instruction code group for executing a predetermined process is associated with the stored branch destination address**," Bates teaches "one embodiment illustrating a method of finding basic block branches of interest is shown as a method 500 in FIG. 5. Method 500 uses the Statement Mapping Table 406 to identify the basic block that contains the program statement number where the program stopped executing. One example of a Statement

Mapping Table 406 is illustrated in FIG. 6. As illustrated, each source line number 602, denoting the program statement of the program being debugged, is referenced to an instruction address 604 locating the source line number in memory and a basic block identifier 606 identifying the basic block that contains the program statement. Referring back to FIG. 5, the method is entered at step 502 where the current statement number, or source line number 602, is retrieved. At step 504, the basic block identifier 606 for the current statement number (source line number 602) is retrieved from the Statement Mapping Table 406. At step 506 a set of all blocks contained in the CDG 300, on which the retrieved basic block identifier 606 is control dependent, is identified and stored in CDSet 158. That is, a set of all blocks reachable along a directed path in the CDG 300 from the block identified by the basic block identifier 606 retrieved at step 504 is stored in the Cdset 158. At step 508 the set of all branches contained in the basic blocks stored in the CDSet 158 is then stored in BranchSet 156. At step 510, a breakpoint is set at each branch stored in BranchSet 156." Accordingly, for at least the statements underlined above, Bates teaches "whether or not an instruction code for calling an instruction code group for executing a predetermined process is associated with the stored branch destination address."

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

> invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-5 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ko (U.S. Pat 6697950 B1) hereinafter referred to as Ko, in view of Bates et al (U.S. Pat Pub 2003/0041315), hereinafter referred to as Bates, as evidenced by Baratloo et al., "Transparent Run-time Defense Against Stack Smashing Attacks," hereinafter referred to as Baratloo.

Re claims 1-5 and 7: Ko teaches a data processing method, a computer program (col 3, lines 56-59), including receiving input data containing a plurality of instruction codes (Figs 1 & 2, elt 108; Fig 3, elts 302 & 304; col 4, lines 37-44 and lines 57-63), and judging whether or not a process executed based on the instruction codes contained in the received data is a malicious process (Fig 3, elt 308; col 5, lines 55-61) said method being characterized by comprising:

However, Bates teaches:

retrieving, an instruction code [current statement] related to a branch instruction [Basic Block B] from the data [process] (Fig 5, elts 502 & 504; ¶48, lines 1-19);

storing a branch origin address [blocks reachable from B] associated with the retrieved instruction code and a branch destination address [BRANCHSET] associated with a branch destination of the instruction code (Fig 5, elts 506, 508 & 510; lines 20-26; ¶51, lines 1-30);

judging whether or not an instruction code for calling an instruction code group for executing a predetermined process is associated with the branch destination address (Fig 5, elt 508; ¶48, lines 20-26); Bates teaches storing the

storing a call destination address of the instruction code if the instruction code is associated with the branch destination address (Fig 5, elt 508; ¶48, lines 20-26);

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teachings of Ko with the teachings of Bates as both references teach tracing through executable code for the purpose of detecting hostile code or instructions. The combination of Ko and Bates is supported by the teachings of Baratloo. Baratloo teaches prevention of “stack smashing”/“buffer overflow” by protecting the stack via canaries (i.e. guards) in the stack; since the stack is used for recalling return addresses and system calls (Abstract; Figs 3, 4 & 5; page 5, right column, ¶3). Analysis of addresses pushed/popped from a program stack is synonymous with tracing through calling/return addresses.

The combination of Ko and Bates teaches judging whether or not the stored call destination address is between the branch origin address and the branch destination address (Ko: Fig 3, elts 304, 306 & 308). The Examiner holds that the branch origin address and branch destination address within a computer program need not have a specific order within a computer program. It is known in the art of computer programming, that function calls could precede the currently executed statement; such practice is common in code which has been obfuscated/scrambled and/or the initial point of execution is obscured as is commonplace in polymorphic and metamorphic code. Ergo, the examiner has interpreted the limitation "judging whether or not the stored call destination address is between the branch origin address and the branch destination address” to mean analyzing any code in an executable program.

The combination of Ko and Bates teaches the information indicating that the data is data for executing a malicious process is outputted (Ko: Fig 3, elt 310).

Conclusion

Examiner's Note: Examiner has cited particular columns and line numbers in the references applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the text of the passage taught by the prior art or disclosed by the examiner.

In the case of amending the claimed invention, Applicant is respectfully requested to indicate the portion(s) of the specification which dictate(s) the structure relied on for proper interpretation and also to verify and ascertain the metes and bounds of the claimed invention.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

JP 09128264 A (a translated copy has been included with this action)

U.S. Pat 6148437 A

U.S. Pat 6775780 B1

U.S. Pat 7340777 B1

U.S. Pat Pub 2002/0083334 A1

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DARREN SCHWARTZ whose telephone number is (571)270-3850. The examiner can normally be reached on 8am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571)272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/D. S./
Examiner, Art Unit 2435
/KimYen Vu/
Supervisory Patent Examiner, Art Unit 2435